1

A Method Of Generating An Authentication

Background and Field of the Invention

5   This invention relates to a method of generating an authentication for updating a mobile communications device's location.

Mobile networking along with the proliferation of wireless devices, such as notebook computers, personal digital assistants and cellular phones are gaining

10   popularity. In mobile networking, a mobile communications device or a mobile device roams between an inter-connected network or inter-network to access or retrieve the desired information and it is imperative that the communication session is not disrupted during the roaming process. When the mobile device roams or switches between networks, its "point of attachment" to the inter-

15   network changes which is invisible to the user since the hand-offs and reconnections occur automatically and seamlessly.

In a typical packet switched inter-network, such as the Internet, data packets are routed from a source inter-network address to a destination inter-network

20   address according to a network number derived from the destination inter-network address by masking off some of the low-order bits. Thus, an inter-network address typically carries information that specifies a device's point of attachment according to the network number. To maintain existing higher-layer connections and to prevent communications breakdown as the mobile device

25   moves from place to place, and thus between networks, the mobile device

should keep its inter-network address the same. However, this is not possible since the correct delivery of packets to the mobile device's current point of attachment depends on the network number contained within the mobile device's inter-network address, which changes at new points of attachment i.e.

5   when the mobile device moves between networks.

If a communications device wishes to send a data packet to the mobile device and is not updated of the new location or point of attachment of the mobile device, the data packet destined for the mobile device may be lost and thus

10   communication would be disrupted. Therefore, to change the routing requires a new inter-network address associated with the new point of attachment.

To overcome the above problem, it has been proposed that the mobile device uses two Inter-network addresses: a home inter-network address (HIA) which is

15   static and used to maintain reachability and connection even when the mobile device is away from the home inter-network, and a care-of inter-network address (CoA) which changes at each new point of attachment and can be regarded as the mobile device's topological significant address. The CoA indicates the new network number and thus identifies the mobile device's point

20   of attachment with respect to the network topology. To maintain continuous network connection, the home network includes a proxy server which receives data messages on behalf of the mobile device and thereafter routes the data message to the mobile device based on the new CoA so that the communications session is not disrupted. The home network proxy server

25   makes it appear that the mobile device is continually receiving data on its home

network but in actual fact, the data is being routed to the new network specified by the CoA.

Alternatively, when the mobile device acquires a new CoA from the new
5   network, the mobile device sends a location update message to its corresponding communications devices informing them of its new CoA. This will allow the corresponding communications devices to send messages using the new CoA to the mobile device. However, upon receiving the update message, a communications device, must verify the authenticity of the location update
10   message before it starts sending messages to the mobile device at the new CoA. Authentication of the location update message is required since a hacker can impersonate the mobile device by sending a location update message with a CoA of his choice such that the corresponding device is bluffed into sending packets to the hacker instead of the mobile device.

15

Most of the authentication methods or protocols in the prior art proposed that the parties concerned pre-share a secret key or recognise each other's public key (see C. Kaufman, R. Perlman, and M. Speciner, *Network Security – Private Communication in A Public World*, PTR Prentice Hall, Englewoor Cliffs, NJ,
20   1995). Sharing a secret key between a mobile device and a random corresponding device in a large inter-connected network such as the Internet is unrealistic and complex. In addition, it is unlikely that a global public key infrastructure over the Internet will take place in the near future.

4

It is an object of the invention to provide a method of generating an authentication which alleviates at least one of the disadvantages of the prior art.

Summary of the Invention

5

In a first aspect of the invention, there is provided a method of generating an authentication for updating a mobile communications device's location to a second communications device, the mobile communications device being registered to a proxy server, the method comprising the steps of, at the time of

10   performing the location update,

i. providing a first input from the proxy server and a second input from the second communications device to a first algorithm to generate a shared secret,

ii. using the shared secret as the authentication when transmitting the

15   location update to the second communications device.

Preferably, the first algorithm is a hash function and the hash of the first and second random numbers is the shared secret.

20   Typically, the mobile communications device has a device address which is part of an inter-network address, the device address is derived from a second algorithm using a cryptographic key associated with the mobile device as the input to the algorithm. Preferably, the second algorithm is a hash function and the hash of the cryptographic key is the device address of the mobile

25   communications device.

In this way, the device address may be used as a form of identification between the second communications device and the proxy server and the mobile communications device may provide the device address and the cryptographic

5 key to the second communications device so that the second communications device can verify the validity of the device address prior to providing the second input to the first algorithm.

Typically, the verification comprises the steps of: performing a hash of the

10 received cryptographic key to obtain a digest, and comparing the digest of the hash function with the received address.

Preferably, the cryptographic key is a public key of an asymmetric key pair associated with the mobile communications device and the method may

15 comprise the step of the second communications device sending an encrypted copy of the second input to the mobile communications device and encrypting the second input using the public key of the mobile device.

Preferably, the shared secret is used as an input to a third algorithm so that an

20 output from the third algorithm is used subsequently as the authentication for updating the location update message. Typically, the third algorithm is a hash function. The authentication may be a hash of the concatenation of the shared secret and the location update message and the method may further comprise the step of transmitting the location update message together with the

25 authentication to the second communications device. On receiving the

authentication and the message, the second communications device may compute a hash of the concatenation of the shared secret and the received location update message for comparison with the received authentication. If the comparison matches, then the second communications device registers the

5   new location of the mobile communications device and transmits any subsequent messages to the new location.

An advantage of the described embodiment of the invention is that the secret is only generated when a need arises to update the new location of the mobile

10 communications device.

Brief Description of the Drawings

An embodiment of the invention will now be described, by way of example, with

15 reference to the accompanying drawings in which,

Figure 1 shows a typical mobile networking system comprising a public network, a home network and a foreign network;

Figure 2 is a flowchart showing the communications between a proxy server

20 residing in the home network of Figure 1 and a corresponding communications for generating a shared secret.

25

Detailed Description of the Preferred Embodiment

It will be appropriate to begin with some background on the concepts and terminology of cryptography. A cryptographic system, or cryptosystem, has an
5   encryption key to transfer plaintext into ciphertext and a decryption key to recover the plaintext from ciphertext. If the encryption key and the decryption key are identical, the cryptosystem is called symmetric key cryptosystem. If the encryption key and the decryption key are different and it is computationally infeasible to determine the decryption key from the encryption key, the
10 cryptosystem is called a public key cryptosystem.

In a public key cryptosystem, anyone can encrypt a message using the public key; however, only the holder of the corresponding private key can decrypt the ciphertext and recover the message.

15

Another form of cryptography is a collision resistant hash function or one-way hash function. Basically, a one-way hash function has the properties that 1) for any message m, it is easy to compute the hash of m which means that it should not take a lot of processing time; 2) given Hash(m), it is computationally
20 infeasible to find message m i.e. a hash algorithm is not reversible; and 3) it is computationally infeasible to find two messages that hash to the same value.

The following notation is used in this application:

$E(M)_{Public}$:encryption of a message M using a public key of a public key
25   cryptographic system;

E(M)$_K$:encryption of a message M using a secret K of a symmetric key cryptographic system

X|Y   :the concatenation of messages X and Y

Hashi()   :a collision resistant one-way hash function, i = 1, 2, 3, 4

5   A->B   :party A sends party B a message

Figure 1 shows a typical mobile networking system comprising a public network 10, a home network 30 and a foreign network 50. The public network 10 is assumed to be insecure and is thus subject to attacks by hackers. The home 10 network 30 comprises a proxy server 20, which is associated with three mobile communications devices 40,41,42 registered with the home network 30 and each mobile device 40,41,42 is assigned a unique home inter-network address (HIA) for identification within the home network 30.

15   Examples of a mobile communications device include portable computers, laptops, PDAs, handheld electronic devices and other suitable devices that communicate wirelessly.

When one of the mobile devices 40 roams or is away from the home network 30 20   and is connected to a foreign network 50, the inter-network address changes since the mobile device 40 acquires a care-of network address (CoA) from the foreign network 50. The mobile device 40 then sends a location update message to the proxy server 20 using a conventional secure communication channel using a pre-shared secret key. The secure channel protects both the 25   integrity and the confidentiality of messages delivered between the mobile

device 40 and the proxy server 20. The mobile device 40 can also send a location update message to all corresponding communications devices 60 in the public network 10 but, as explained earlier, the corresponding communications device 60 needs some form of assurance that the location update message is indeed from the mobile device 40 before accepting the change since a hacker may have sent the update message impersonating the mobile device 40.

A corresponding communications device, in the context of this application, includes a server, a personal computer or another mobile communications device.

The authenticity of the location update messages from mobile device 40 needs to be verified by the corresponding device 60 before the corresponding device 60 can register the new location of the mobile device 40. The following embodiment describes how to authenticate a location update message efficiently without any pre-defined security associations between the corresponding device 60 and the mobile device 40 or the proxy server 20.

To enhance the network security, the proxy server 20 and the mobile device 40 may use an asymmetric key pair or a pre-shared secret key for encrypting messages transmitted between the proxy server 20 and the mobile device 40. In this way, a secure channel is achieved between the mobile device 40 and the proxy server 20.

10

As mentioned earlier, the HIA comprises the network number (Net_MD) which identifies which network the mobile device 40 is currently attached. The HIA also comprises the host address (Host_MD) which identifies the mobile device 40 uniquely in the home network. The HIA can thus be represented by:

5   HIA_MD = Net_MD | Host_MD

Since the public key associated with a mobile device is also unique, the public key can be used to identify the mobile device 40. Therefore the Host_MD can be derived from the public key. In this example, a hash of the public key is used to represent the Host_MD i.e. Host_MD = $Hash1(MD_{public})$.

10

When a corresponding device 60 intends to send a data packet or message to the mobile device 40, the corresponding device 60 first checks its local cache to see if there is a location update entry, which has been authenticated previously, for the mobile device 40. If there is an authenticated valid entry, the

15   corresponding device 60 sends the data packet to the CoA of the mobile device 40. If there is no location update entry, the corresponding device 60 and the proxy server 20 would engage in a message exchange as shown in Figure 2.

At step 100, the corresponding device 60 sends a data packet PAC to the

20   mobile device's 40 HIA. When the packet PAC arrives at the mobile device's home network 30, the packet PAC would be received by the proxy server 20 at step 110. At step 120, the proxy server 20 checks to see if the mobile device 40 is residing in the home network 30. If the mobile device 40 is in the home network 30, the packet PAC will be delivered to the mobile device 40 at step

25   130 and the process ends.

On the other hand, if the mobile device 40 is not located in the home network 30 the proxy server 20 initiates a "key setup protocol" with the corresponding device 60 at steps 140 and 150 of Figure 2. Note that the proxy server 20 would

5   have been notified of the new CoA of the mobile device 40 since the mobile device 40 would update the proxy server 20 whenever the CoA changes.

The key setup protocol makes use of a binding relationship between the public key MD_{public} and the HIA of the mobile device 40:

10   $HIA\_MD = Net\_MD \mid Host\_MD$, where Net_MD is the network number of the home 30 to which the mobile device 40 is connected and $Host\_MD = Hash1(MD_{public})$. The result of running the key setup protocol is that the home server 20 and corresponding device 60 share a secret K.

15   The example for this embodiment is a public key cryptosystem and thus the key setup protocol will be as follows:

1) HS -> CD: $M1 = HIA\_MD \mid MD_{public} \mid R1 \mid NetMask$

2) CD -> MD: $M2 = E(MD_{public}, R1, R2)$

20   3) HS -> CD: $M3 = Hash3(K \mid M1 \mid M2 \mid K)$

The first step in the key setup protocol is initiating the key setup and this takes the form of the proxy server 20 sending a message M1 to the corresponding device 60. In this embodiment, the message M1 also consists of the inter-

25   network address HIA_MD of the mobile device 40, the public key MD_{public}, and a

12

random number R1 generated by the proxy server 20 and a Network Mask NetMask. The random number R1 acts as a challenge from the proxy server 20 to the corresponding device 60.

5   Upon receiving the message M1, the corresponding device 60 uses the network mask NetMask to extract the network number Net_MD and the host address Host_MD from the inter-network address HIA_MD. The corresponding device 60 then computes the digest of $Hash1(MD_{public})$ and compares the digest with the actual host address Host_MD. If the comparison is different, the

10   corresponding device 60 terminates the process. On the other hand, if the comparison is the same, the corresponding device 60 will know that the MD_{public} is the public key associated with the mobile device's 40 home inter-network address HIA_MD.

The corresponding device 60 then proceeds to generate a second random

15   number R2 and computes a secret K whereby $K = Hash2(R1 \mid R2)$, i.e. K is the hash of the concatenation of the two random numbers R1 and R2.

The corresponding device 60 then encrypts R2 using the mobile device's 40 public key MD_{public} and sends a message $M2 = E(MD_{public}, R2)$ to the HIA of the

20   mobile device 40. When the message M2 arrives at the home network 30, the message M2 is again intercepted by the proxy server 20 which decrypts M2 using the corresponding private key $MD_{private}$ of the public key cryptosystem to obtain R2 and similarly computes the secret K using the same hash algorithm i.e. $Hash2(R1 \mid R2)$.

25

At this stage, the secret K is generated using the two random numbers R1 and R2 contributed by the proxy server 20 and the corresponding device 60 respectively. The proxy server 20 then sends an authentication code to the corresponding device 60. The authentication code can take the form of a third message M3 whereby M3 = Hash3(K | M1 | M2 | K) and the message M3 is then sent to the corresponding device 60. In this example, the secret K is concatenated to both the front and the back of the messages M1 and M2 (which were transmitted previously to the corresponding device 60) and this serves to enhance the strength of the digest of the hash algorithm.

Upon reception of the message M3, the corresponding device 60 proceeds to compute the digest of Hash3(K | M1 | M2 | K) separately and compares it with the received message M3. Since the message M3 functions as a message authentication code, the digest can only be computed and verified by a party who knows the secret K. Therefore, if the digest computed by the corresponding device 60 is the same as the received message M3 then the corresponding device 60 will know that the mobile device 40 (and the proxy server 20) has received the secret K and will use the secret K for authenticating a location update message from the mobile device 40 in subsequent communications. Alternatively, if the digest computed from the hash and the received message M3 is different, then the corresponding device 60 will terminate the communication.

Note that as far as corresponding device 60 is concerned, the key setup protocol was performed with the mobile device 40 since the HIA of the mobile

14

device 40 was used as the destination address. In fact, the key setup was performed with the proxy server 20 functioning as a security proxy for the mobile device 40 which is transparent to the corresponding device 60.

5. Having obtained the secret K, this will be used between the mobile device 40 and corresponding device 60 to authenticate location update messages, as will be described below.

Referring to Figure 2 again, at step 160, the proxy server 20 forwards the data

10 packet PAC received from the corresponding device 60 and forwards the packet PAC together with the secret K using the pre-defined secured medium to the mobile device 40. Note that it is imperative that the confidentiality of K must be protected during the delivering process from the proxy server 20 to the mobile device 40.

15

After receiving the packet PAC and the secret K, the mobile device 40 extracts the corresponding device's 60 inter-network address IA_CD from the data packet PAC and computes a location update message as follows:

M4 = HIA_MD | CoA_MD | IA_CD | INTV, COUNT, MAC

20 where CoA_MD is the mobile device's 40 new care-of inter-network address, INTV is the maximum valid interval which a corresponding device 60 can send data to the CoA_MD, COUNT is a counter which is used to counter reply of the message to detect replay of location update messages by a hacker, and MAC = message authentication code. The MAC in this example is in the following form:

25 Hash4(K | HIA_MD | CoA_MD | IA_CD | INTV, COUNT)

The mobile device 40 then sends the location update message M4 (which also includes the message authentication code) to the corresponding device 60. Upon receiving the message M4, the corresponding device 60 checks the

5   validity of the message using the MAC as reference. Similar to the previous Hash digest, the corresponding device 60 proceeds to use the received message HIA_MD | CoA_MD | IA_CD | INTV, COUNT, minus the MAC, and separately computes the digest of the Hash4 function using its own secret K which has been calculated previously during the key setup process with the

10   proxy server 20. If both digest are the same then the corresponding device 60 knows that the location update message is indeed valid and that the message came from the mobile device 40 and can safely update the mobile device's 40 CoA location in the location update cache table by recording the binding of the HIA_MD and the new CoA_MD, as well as the associated interval INTV. The

15   authentication procedure is then completed. From this point on, the corresponding device 60 can continue to communicate with the mobile device 40 by sending messages directly to the mobile device's CoA_MD.

Using the above described embodiment, an advantage is that the secret K is

20   generated when a need arises to update the new CoA of the mobile device 40. If the mobile device 40 roams to a different network such that the CoA changes again, the same procedure may be utilised to generate a new secret K since the corresponding device 60 and the proxy server 20 may provide a new input to generate a new random number. Therefore a new secret K can be used for the

25   message authentication code thus enhancing the security of the mobile network

system. Alternatively, since a secret key is already shared between the mobile device 40 and the corresponding device 60, the same secret key can be used to authenticate future location update messages which is more efficient.

5   The described embodiment should not be construed as limitative. For example, the secret K can be appended before and/or after a message when performing a hash algorithm using the secret as an input. After the key setup process and obtaining the secret K, the proxy server can proceed to update the CoA of the mobile device 40 by performing the same authentication procedure instead of

10   sending the secret K to the mobile device 40.

Having now fully described the invention, it should be apparent to one of ordinary skill in the art that many modifications can be made hereto without departing from the scope as claimed.

15